

Nutzerzertifikat beantragen

Für die Beantragung Ihres persönlichen Zertifikates haben wir schon alles vorbereitet. Bitte beachten Sie folgende Hinweise:

Hinweis: Während des Verfahrens erhalten Sie eine E-Mail. Diese E-Mail wird *grundsätzlich* an Ihre *FH - E-Mailadresse* geschickt. Wenn eine Weiterleitung dafür eingerichtet ist, achten Sie bitte darauf, dass diese auch Mails akzeptiert und Sie Zugriff darauf haben! Die Weiterleitung kann von Studierenden im [Virtuellen Service-Center](#) unter "Mein Studium"->"Adresse ändern" selbst kontrolliert und bearbeitet werden.

Hinweis: Wir empfehlen die Beantragung mit einem [Mozilla-Browser](#) (z.B. Firefox) durchzuführen, weil hier das Speichern des Zertifikates direkt im eToken problemlos möglich ist. Außerdem verhalten sich diese Browser auf allen getesteten Betriebssystemen gleich. Die spätere Nutzung des Zertifikates ist natürlich auch mit dem IE möglich.

Hinweis: Als Mozilla-/Firefox-Nutzer installieren Sie bitte durch Klick die folgenden CA-Zertifikate:

[FH-SWF CA](#)

[DFN-Verein CA Services](#)

Sie werden dabei gefragt, ob und für welche Zwecke Sie das jeweilige CA-Zertifikat installieren möchten. Kreuzen Sie alle 3 Optionen an und bestätigen Sie mit "OK".

Besuchen Sie nun unsere Zertifizierungsstelle ([CA-Server](#)) und wählen Sie in der Rubrik "Self-Service" den Punkt "Zertifikat beantragen":

Fachhochschule Südwestfalen
Hochschule für Technik und Wirtschaft
University of Applied Sciences

Self-Service CA-Zertifikate Policies Hilfe

Zertifikat beantragen Zertifikat sperren Zertifikat suchen

Nutzerzertifikat beantragen

Bitte geben Sie Ihren Nutzernamen und Ihr Passwort ein. Felder mit Stern (*) müssen ausgefüllt werden.

Nutzername * sttatest

Passwort * [masked]

Ich stimme der **Zertifizierungsrichtlinie** zu. *

Ich stimme der Veröffentlichung des Zertifikats zu.

Wenn Sie der Veröffentlichung nicht zustimmen, wird Ihr Zertifikat nicht im Verzeichnisdienst zur Verfügung stehen.

Weiter

Melden Sie sich mit Ihrer Benutzerkennung und Ihrem ERST-Passwort an.

Hinweis: Wenn Sie der Veröffentlichung Ihres Zertifikates nicht zustimmen, werden Sie beim späteren Import nach einer "PIN" gefragt. Diese PIN ist Ihr Erstpasswort.

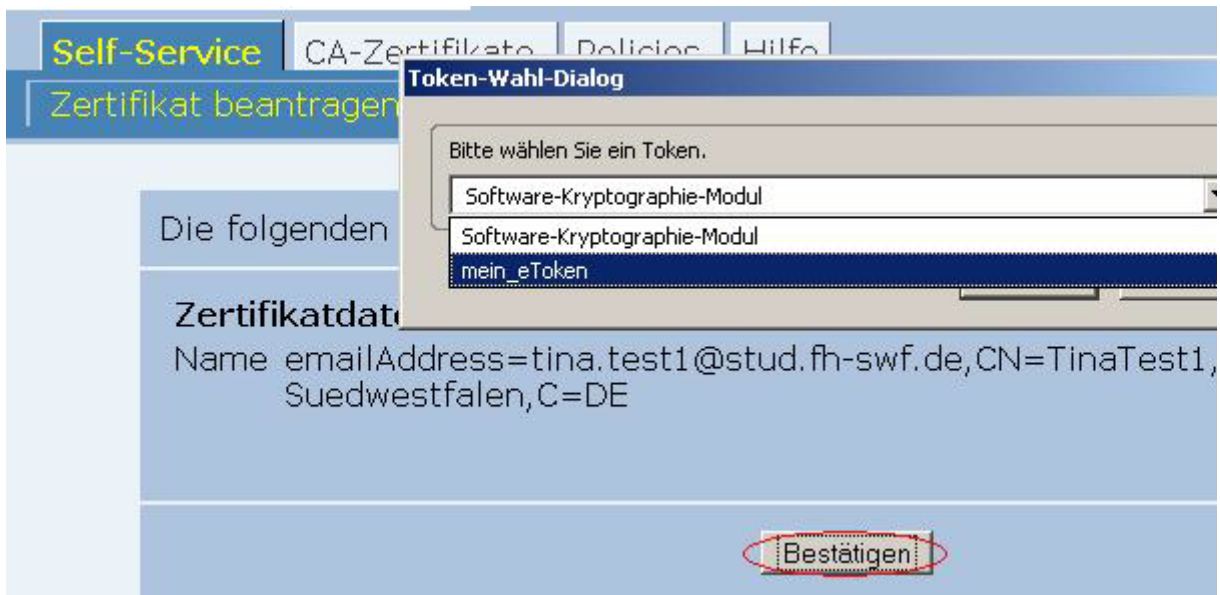
Nach dem Klick auf "Weiter" öffnet sich ein Fenster mit den persönlichen Daten. Diese bestätigen Sie.

Es wird nun Ihr *persönlicher* Schlüssel generiert.

Die Anwendung fragt nach dem Speicherort - in diesem Fall wird der **angeschlossene eToken** ausgewählt.

Bitte beachten Sie:

Der persönliche Schlüssel darf, wie der Name vermuten lässt, **niemals** weitergegeben werden. Zum späteren Import Ihres Zertifikates benötigen Sie diesen persönlichen Schlüssel. Also können Sie Ihr Zertifikat nur dort importieren, wo Ihr persönlicher Schlüssel zur Verfügung steht (also im eToken oder in der Anwendung).



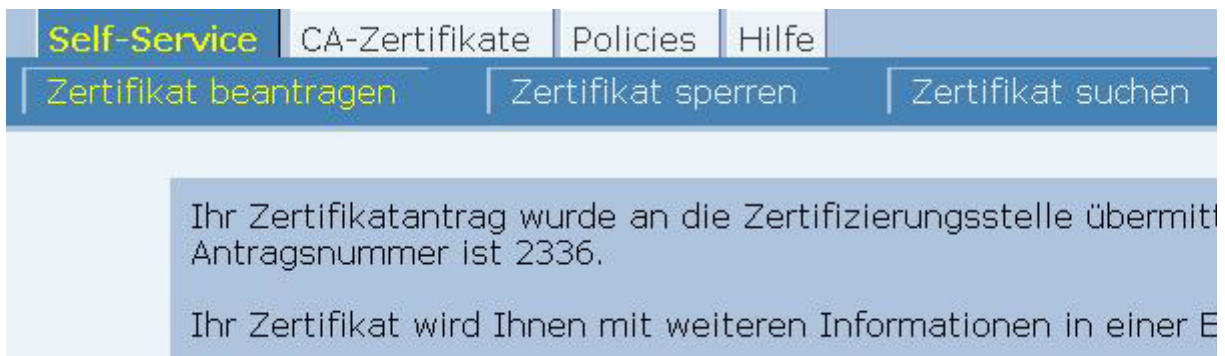
Da der eToken passwortgeschützt ist, erscheint folgender Dialog:



Geben Sie das Master-Passwort des eToken ein und bestätigen Sie mit "OK". Falls Sie es noch nicht geändert haben, lautet es "1234567890". Wir empfehlen aber unbedingt ein eigenes Passwort zu vergeben (Siehe "Softwarefunktionen").

Die Generierung des Schlüssels nimmt nun einige Sekunden in Anspruch.

Anschließend wird Ihnen eine E-Mail zum weiteren Vorgehen zugesandt.



Hiermit ist der erste Schritt abgeschlossen. Warten Sie nun den Erhalt der E-Mail ab, welcher in der Regel nach wenigen Minuten erfolgt.

In der E-Mail sind unter anderem 2 Links angegeben. Der 1. Link beschreibt den Import des

CA- und Wurzelzertifikates.

Über den 2. Link importieren Sie Ihr persönliches Zertifikat in den eToken:



Das Zertifikat wird nun im eToken gespeichert, es muss also nicht zusätzlich gesichert werden.